AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Previously Presented) A computer system, comprising:

a chipset;

an internal component of the computer system;

a bus coupled to the chipset to communicate a trusted data cycle to the internal component of the computer system;

a docking connector; and

a secured docking circuit coupled to the bus and coupled between the bus and the docking connector to scan for the trusted data cycle, detect the trusted data cycle, and provide a filtering mechanism to prevent the trusted data cycle from being provided to a device external to the computer system through the docking connector.

2. (Original) The computer system of claim 1, wherein the bus is a Low Pin Count bus.

3. (Original) The computer system of claim 1, wherein the component provides protected memory storage.

4. (Original) The computer system of claim 1, wherein the component provides platform authentication.

5. (Original) The computer system of claim 1, wherein the component maintains a protected path between the chipset and a keyboard.

6. (Original) The computer system of claim 1, wherein the computer system is a notebook computer.

7. (Previously Presented) A circuit, comprising:

means for transmitting data on a Low Pin Count (LPC) bus; and

filtering means for scanning for trusted data cycles on the Low Pin Count (LPC) bus and preventing the trusted data cycles on the Low Pin Count (LPC) bus from being accessed by an unauthorized component coupled to a docking connector, wherein the filtering means is between the Low Pin Count (LPC) bus and the docking connector.

8. (Cancelled)

9. (Original) The circuit of claim 7, further comprising:

means for monitoring data cycles on the LPC bus.

10. (Previously Presented) A method, comprising:

monitoring for communication of trusted data cycles on a bus with a secured docking logic of a computer system, the secured docking logic coupled between the bus and a docking connector;

detecting each of the trusted data cycles by detecting a predefined trusted data cycle indicator with the secured docking logic; and

preventing the trusted data cycles from being available to a component external to the computer system with the secured docking logic.

11. (Previously Presented) The method of claim 10, wherein the trusted data cycles begin with a "0101" value.

12. (Previously Presented) The method of claim 10, further comprising:

communicating trusted data cycles between a chipset of the computer system and a first component of the computer system that provides cryptographic capabilities.

13. (Previously Presented) The method of claim 12, wherein the communication of the trusted data cycles between the chipset and the first component is in plaintext format.

14. (Previously Presented) The method of claim 10, further comprising:

communicating trusted data cycles between a chipset of the computer system and a second component of the computer system that provides trusted input capabilities.

15. (Previously Presented) The method of claim 14, wherein the communication of the trusted data cycles between the chipset and the second component is in plaintext format.

16. (Original) The method of claim 15, wherein the second component maintains a protected path between the chipset and a keyboard, wherein keystroke data is communicated by the chipset to protected memory and trusted applications.

17. (Original) The method of claim 15, wherein the second component maintains a protected path between the chipset and a mouse, wherein pointer data from the mouse is communicated by the chipset to protected memory and trusted applications.

18. (Original) The method of claim 12, wherein the first component protects secret data of the computer system by encrypting the secret data.

19. (Original) The method of claim 18, wherein the secret data is decrypted by hardware of the computer system.

20. (Previously Presented) The method of claim 18, wherein the first component merges data with configuration values of the computer system.

21. (Original) The method of claim 18, wherein the first component requests for a system identification request.

22. (Previously Presented) The method of claim 21, wherein a trusted third party chip verifies an identification of the computer system and sends a response to the first component.

23. (Previously Presented) The computer system of claim 1, wherein the circuit makes a data cycle that is not a trusted data cycle available to the device external to the computer system.

24. (Previously Presented) The computer system of claim 1, wherein if the circuit determines that a data cycle is not a trusted data cycle the circuit does not prevent the device external to the computer system from accessing the data cycle.

25. (Previously Presented) The computer system of claim 1, wherein the circuit blocks the trusted data cycle from the docking connector.

26. (Previously Presented) The computer system of claim 1, wherein the trusted data cycle begins with a predefined trusted data cycle indicator.

27. (Previously Presented) The method of claim 10, wherein preventing comprises filtering to block the trusted data cycles without blocking data cycles that are not trusted data cycles.

28. (Previously Presented) The computer system of claim 1, wherein the trusted data cycle comprises a trusted data cycle indicator and plaintext format data.

29. (Previously Presented) A system comprising:

a chipset;

a first internal component to provide at least one hardware cryptographic functionality selected from hardware protected storage, platform binding, and platform authentication;

a second internal component to provide a trusted input capability from a keyboard;

a bus coupled to the chipset, coupled to the first internal component, and coupled to the second internal component, the bus to communicate a trusted data cycle from the chipset to the first internal component;

a docking connector; and

secured docking logic coupled between the bus and the docking connector, the secured docking logic to block the trusted data cycle from an external device coupled with the docking connector.

30. (Previously Presented) The system of claim 29, wherein the trusted data cycle comprises a trusted data cycle indicator and data in a plaintext format.

31. (Previously Presented) The system of claim 30, wherein the trusted data cycle indicator comprises 0101.

32. (Previously Presented) The system of claim 29, wherein the secured docking logic comprises a circuit.